CLAIMS

1. A computer controlled method comprising:

establishing communication between a provisioning device and a network device over a preferred channel;

exchanging key commitment information over said preferred channel between said provisioning device and said network device to pre-authenticate said network device; and

providing provisioning information to said network device over said preferred channel, whereby said network device can automatically configure itself for communication over a network responsive to said provisioning information.

2. The computer controlled method of claim 1, wherein said provisioning information comprises network configuration information.

3. The computer controlled method of claim 1, further comprising

receiving a public key from said network device;

verifying said public key with said key commitment information; and

automatically provisioning said network device with a credential authorized by a credential issuing authority.

4. The computer controlled method of claim 3, further comprising establishing proof that said network device is in possession of a private key corresponding to said public key.

5. The computer controlled method of claim 3, wherein said credential issuing authority is a certification authority and said credential is a public key certificate.

6. The computer controlled method of claim 3, wherein the step of automatically provisioning is responsive to authorization from a registration agent.

7. The computer controlled method of claim 1, wherein said preferred channel is a location-limited channel.

8. The computer controlled method of claim 1, wherein said preferred channel has a demonstrative identification property and an authenticity property.

9. The computer controlled method of claim 1, wherein the network is a wireless network, and wherein said provisioning device is a wireless access point.

10. The computer controlled method of claim 9, further comprising:

receiving a wireless communication;

determining whether said wireless communication originated from said network device or from a second network device that was not provisioned by said wireless access point; and

routing said wireless communication responsive to the step of determining.

11. The computer controlled method of claim 10, wherein the step of routing comprises:

choosing a selected channel from a secure channel and an insecure channel responsive to the step of determining; and

sending said wireless communication through said selected channel.

12. The computer controlled method of claim 1, wherein said provisioning device is in communication with a credential issuing authority.

13. A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method to provision a network device, the method comprising steps of:

establishing communication between a provisioning device and said network device over a preferred channel;

exchanging key commitment information over said preferred channel between said provisioning device and said network device to pre-authenticate said network device; and

providing provisioning information to said network device over said preferred channel, whereby said network device can automatically configure itself for communication over a network responsive to said provisioning information.

14. The computer-readable storage medium of claim 13, further comprising

receiving a public key from said network device;

verifying said public key with said key commitment information; and

automatically provisioning said network device with a credential authorized by a credential issuing authority.

15. The computer-readable storage medium of claim 13, wherein the network is a wireless network, and wherein said provisioning device is a wireless access point.

16. An apparatus for provisioning a network device comprising:

at least one port configured to establish a preferred channel;

a preferred communication mechanism configured to be able to establish communication with and said network device over said preferred channel;

a pre-authentication mechanism configured to be able to receive key commitment information over said preferred channel from said network device; and

a provisioning mechanism configured to be able to provide provisioning information to said network device over said preferred channel, whereby said

network device can automatically configure itself for communication over a network responsive to said provisioning information.

17. The apparatus of claim 16, wherein said provisioning information comprises network configuration information.

18. The apparatus of claim 16, further comprising

a key reception mechanism configured to receive a public key;

a key verification mechanism configured to verify said public key with said key commitment information; and

a credential provisioning mechanism configured to automatically provide a credential authorized by a credential issuing authority.

19. The apparatus of claim 18, further comprising a key exchange mechanism configured to be able to perform a key exchange protocol with said network device.

20. The apparatus of claim 18, wherein said credential issuing authority is a certification authority and said credential is a public key certificate.

21. The apparatus of claim 16, wherein said preferred channel is a location-limited channel.

22. The apparatus of claim 16, wherein the network is a wireless network, and the apparatus further comprises a wireless access point mechanism.

23. The apparatus of claim 22, further comprising:

a packet receiver mechanism configured to receive a wireless communication;

a determination mechanism configured to determine whether said wireless communication received by the packet receiver mechanism originated from said network device or from a second network device that was not provisioned by said wireless access point; and

a router mechanism configured to route said wireless communication responsive to the determination mechanism.

24. The apparatus of claim 23, wherein the router mechanism further comprises:

a channel selection mechanism configured to choose a selected channel from a secure channel and an insecure channel responsive to the determination mechanism; and

a transmission mechanism configured to send said wireless communication through said selected channel.

25. The apparatus of claim 16, further comprising a non-preferred communication mechanism that can be used to communicate with a credential issuing authority.

26. A computer controlled method comprising:

establishing communication between a network device and a provisioning device over a preferred channel;

receiving provisioning information from said provisioning device over said preferred channel;

exchanging key commitment information over said preferred channel between said provisioning device and said network device to pre-authenticate said network device; and

automatically configuring said network device for communication over a network responsive to said provisioning information.

27. The computer controlled method of claim 26, further comprising executing a key exchange protocol.

28. The computer controlled method of claim 27, further comprising establishing a communication channel between said network device and a credential issuing authority responsive to the step of executing wherein said communication channel is secure.

29. The computer controlled method of claim 26, wherein the network is a wireless network, said provisioning device is a wireless access point, and wherein said provisioning information comprises a service set identifier (SSID).

30. The computer controlled method of claim 29, wherein the network is a wireless network, said provisioning device is a wireless access point, and wherein said provisioning information comprises a privacy key.

31. The computer controlled method of claim 26, wherein said provisioning information comprises a credential.

32. The computer controlled method of claim 26, further comprising

receiving a public key from said provisioning device;

verifying said public key with said key commitment information; and

automatically provisioning said network device with a credential authorized by a credential issuing authority.

33. The computer controlled method of claim 32, wherein the network is a wireless network, said provisioning device is a wireless access point, and wherein said provisioning information comprises a service set identifier (SSID).

34. The computer controlled method of claim 33, wherein the network is a wireless network, said provisioning device is a wireless access point, and wherein said provisioning information comprises a privacy key.

35. The computer controlled method of claim 32, wherein said provisioning information comprises network configuration information.

36. The computer controlled method of claim 32, wherein the step of automatically provisioning is responsive to authorization from a registration agent.

37. The computer controlled method of claim 32, wherein said credential issuing authority is a certification authority and said credential is a public key certificate.

38. The computer controlled method of claim 26, wherein said preferred channel is a location-limited channel.

39. The computer controlled method of claim 26, wherein said preferred channel has a demonstrative identification property and an authenticity property.

40. The computer controlled method of claim 26, wherein said network device is from one or more of the group consisting of a computer, a personal data assistant, a smart card, a cryptographic token, a medical device, a device containing personal information, a secure telephone, a cell telephone, a vehicle, a container, an access card, a biometric sensor, a wireless network device, a proximity sensor, a sensor device, traffic sensor, an alarm device, a robot, a device capable of receiving a credential, a device capable of issuing a credential.

41. A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method to automatically provision a network device, the method comprising steps of:

establishing communication between said network device and a provisioning device over a preferred channel;

receiving provisioning information from said provisioning device over said preferred channel;

exchanging key commitment information over said preferred channel between said provisioning device and said network device to pre-authenticate said network device; and

automatically configuring said network device for communication over a network responsive to said provisioning information.

42. The computer-readable storage medium of claim 41, wherein said preferred channel has a demonstrative identification property and an authenticity property.

43. The computer-readable storage medium of claim 41, wherein said network device is from one or more of the group consisting of a computer, a personal data assistant, a smart card, a cryptographic token, a medical device, a device containing personal information, a secure telephone, a cell telephone, a vehicle, a container, an access card, a biometric sensor, a wireless network device, a proximity sensor, a sensor device, traffic sensor, an alarm device, a robot, a device capable of receiving a credential, a device capable of issuing a credential.

44. An apparatus comprising:

at least one port configured to establish a preferred channel;

a preferred channel communication mechanism configured to be able to establish communication with a provisioning device over said preferred channel;

a receiver mechanism configured to be able to receive provisioning information from said provisioning device over said preferred channel;

a pre-authentication mechanism configured to be able to receive key commitment information over said preferred channel from said provisioning device; and

a communication setup mechanism configured to automatically configure the apparatus for communication over a network responsive to said provisioning information received by the receiver mechanism.

45. The apparatus of claim 44, wherein said provisioning information comprises network configuration information.

46. The apparatus of claim 44, wherein the network is a wireless network, said provisioning device is a wireless access point, and wherein said provisioning information comprises a service set identifier (SSID).

47. The apparatus of claim 44, wherein said provisioning information comprises a credential.

48. The apparatus of claim 44, further comprising a key exchange mechanism configured to execute a key exchange protocol.

49. The apparatus of claim 44, further comprising

a key reception mechanism configured to receive a public key;

a key verification mechanism configured to verify said public key with said key commitment information; and

a credential receiver mechanism configured to receive a credential authorized by a credential issuing authority.

50. The apparatus of claim 49, wherein the credential receiver mechanism is capable of being responsive to authorization from a registration agent.

51. The apparatus of claim 49, wherein the network is a wireless network, said provisioning device is a wireless access point, and wherein said provisioning information comprises a service set identifier (SSID).

52. The apparatus of claim 51, wherein the network is a wireless network, said provisioning device is a wireless access point, and wherein said provisioning information comprises a privacy key.

53. The apparatus of claim 49, wherein said credential issuing authority is a certification authority and said credential is a public key certificate.

54. The apparatus of claim 44, wherein said preferred channel is a location-limited channel.

55. The apparatus of claim 44, wherein the apparatus is from one or more of the group consisting of a computer, a personal data assistant, a smart card, a cryptographic token, a medical device, a device containing personal information, a secure telephone, a cell telephone, a vehicle, a container, an access card, a biometric sensor, a wireless network device, a proximity sensor, a sensor device, traffic sensor, an alarm device, a robot, a device capable of receiving a credential, a device capable of issuing a credential.